WHAT IS CLAIMED IS:

1. An electronic module used for secure transactions comprising:

input/output circuitry for communicating to a data processing circuit;

math coprocessor circuitry electrically connected to said input/output circuitry;

microprocessor circuitry electrically connected to said input/output circuitry; and

memory circuitry electrically connected to said microprocessor circuitry, said electronic module being programmable to provide secure, encrypted data transfers between said electronic module and said data processing circuit.

2. The electronic module of claim 1, wherein said data processing circuit is another electronic module.

3. The electronic module of claim 1, further comprising a one-wire interface connected to said input/output circuitry.

4. The electronic module of claim 1, wherein said memory circuitry is adapted to store a private encryption/decryption key for use during the encrypted data transfers between said electronic module and said data processing circuit..

5. The electronic module of claim 1, wherein said encrypted transactions are time stamped.

6. A system for communicating secure transactions, comprising:

a first module comprising:

input/output circuitry;

random number creating means for creating a random number; and

a first transaction group for requesting said random number creating means to create said random number and for providing said random number to said input\output circuitry; and

a service provider equipment comprising:

means for reading said random number from said input/output circuitry of said first module;

means for combining said random number with a first data and for encrypting the combination of said random number and said first data with a private key to produce a first certificate, whereby said input/output circuity of said first module is adapted to receive said first certificate.

7. The system of claim 6, wherein said service provider equipment comprises a second module.

8. The system of claim 6, wherein said first module further comprises an identifier for identifying said first module, and wherein said first transaction group provides said identifier to said input/output circuitry.

9. The system of claim 8, wherein said means for reading is further for reading said identifier from said input/output circuitry of said first module.

10. The system of claim 6, wherein said first module further comprises a second transaction group.

11. The system of claim 6, wherein said module further comprises a means for time stamping a complete transaction.

12. A method of communicating encrypted information between a module and a service provider equipment, comprising the steps of:

a) creating a first random number in said module;

b) passing said random number to said service provider equipment;

c) encrypting at least said random number with a private key in said service provider equipment thereby producing a certificate;

d) passing at least said certificate to said module;

e) decrypting said certificate with a public key in said module;

f) comparing said first random number with a number found in the decrypted first certificate of step e) to determine if the two numbers match.

13. The method of claim 12, wherein step b) further comprises the step of passing a module identifier to said service provider equipment.

14. The method of claim 12, wherein said service provider equipment is another module.

15. The method of claim 12, wherein said method incorporates a single wire bus.

16. The method of claim 15, wherein said single wire bus is substantially a one-wire bus.

17. A method of communicating encrypted information between a module and a service provider equipment, comprising the steps of:

a) creating a first random number in said service provider equipment;

b) passing said random number to said module;

c) encrypting at least said random number with a private key in said module thereby producing a first certificate;

d) passing at least said first certificate to said service provider equipment;

e) decrypting said first certificate with a public key in said service provider equipment;

f) comparing said first random number with a number found in the decrypted first certificate of step f) to determine if the two numbers match.

18. The method of claim 17, wherein said service provider equipment is another module.

19. The method of claim 17, wherein said method incorporates a single wire bus.

20. The method of claim 17, wherein said single wire bus is substantially a one-wire bus.

21. A method of decrypting encrypted data using a module, comprising the steps of:

receiving a first encrypted data and a second encrypted data;

~~decrypting said first encrypted data with a private key stored in said module, whereby a first decryption key is created;~~

~~providing said first decryption key to an electronic system;~~

~~decrypting said second encrypted data with said first decryption key via said electronic system, whereby a useful information is created.~~

~~22. The method of claim 21, wherein said encrypted data is an electronic mail message.~~

Add A2

Add B1

Add C1